Ex. 18
Wenke Lee Rebuttal Opinion Summaries

[redacted]

II. SUMMARY OF FINDINGS

5. First, I consider the four aspects of Apple's iOS security model identified by Professor Rubin—identity verification of developers, manual and automated app review processes, certificate validation and code-signing, and on-device security protections. I find that none of these aspects of Apple's iOS security model requires an exclusive app distribution model. Third parties could perform each of these security aspects, except for Apple's on-device security protections, which are independent of the app distribution channel. Alternatively, Apple itself could continue to provide developer verification, malware screening, notarization and code signing, just as it does on the macOS platform today, even with its adoption of a more open app distribution model. Lastly, permitting third-party distribution channels on iOS would not weaken on-device iOS security protections.

6. Second, I find that Apple could continue to offer users the option to have the same level of security that they currently receive through the iOS App Store in a more open distribution model. Additionally, in a more open distribution model, developers could use channels, other than the iOS App Store, to distribute native iOS apps[2] that have been screened for security issues[3] and signed, and therefore offer a comparable (or even better in instances where third-party reviewers develop innovative security screening techniques) level of security as apps distributed through the iOS App Store. Developers could also use alternative channels to distribute native iOS apps that have not been signed or screened by a third party for security issues; users who choose to download apps through such channels would still receive the benefit of the protection provided by on-device iOS security features. Apple's on-device security features are designed to ensure that the impact of any malware downloaded onto an iOS device remains localized.

[2] When I describe "native iOS apps," I am referring to apps that directly run on the operating system, as opposed to those that run through additional middleware (i.e., browser) on top of the operating system. Native apps can be developed by both Apple and third parties.

[3] When I reference "security screens" or "screens for security issues," I refer to the six different security screening steps that I identified in my first expert report and found that third parties could perform. For more information, see Section V.E of my first expert report.

[redacted]

7. Third, I find that Professor Rubin fails to adequately justify why Apple's macOS distribution model is inappropriate for iOS. Contrary to what Professor Rubin suggests, macOS devices contain similarly sensitive user data to iOS devices; further, data is often automatically synchronized between iOS and macOS devices via iCloud. As a result, iOS and macOS have similar data security considerations.

8. Finally, I find that third parties, such as Square and Stripe, have built secure in-app payment systems for iOS. In fact, purchases of physical goods and services on iOS already use such third-party payment systems. Apple already contracts with third-party payment settlement platforms to facilitate Apple's IAP transactions. While Apple may have unique access to on-device user data and hardware that it can use to compute fraud scores and biometrically authenticate each in-app purchase, third-party payment settlement providers frequently detect fraud based on more extensive datasets and can use Apple's public APIs to biometrically authenticate users.